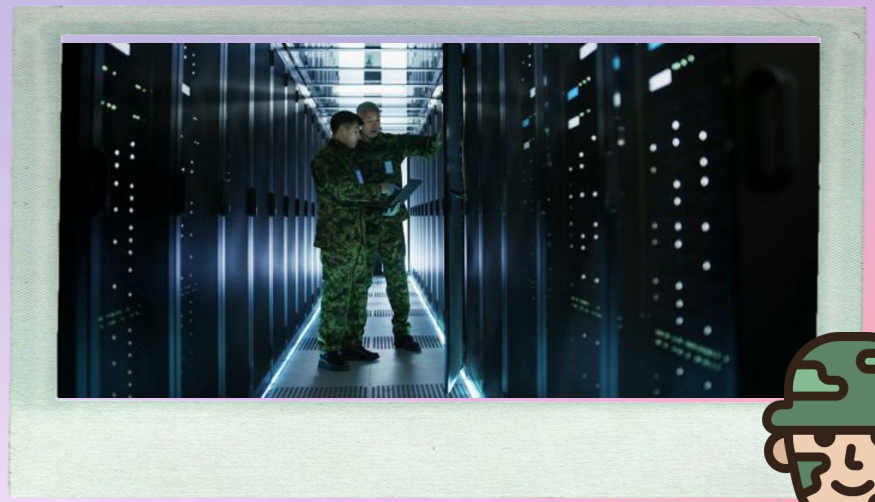
Sentinel

<Delve into Web Dev>

DEFENDING OUR DIGITAL WAY OF LIFE

From Caesar to Today

In the past, encryption was a game played by the great Armies for military purposes



From Caesar to Today

With the advent of modern computing, businesses wanted to secure their digital data from competitors

Nowadays encryption is used by everyone everywhere to secure their data!

Cryptography Today

Almost all internet traffic today is encrypted! (HTTPS)

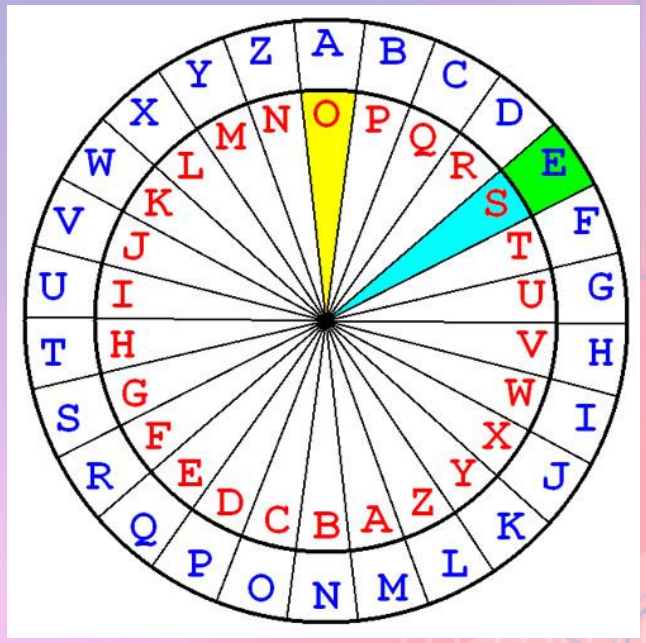
Your WhatsApp messages are End-to-End encrypted

All of the files on your phone are encrypted

The data that you store on the cloud is encrypted

Modern Cryptography

Actually, modern cryptography is not very different from the ciphers we studied in this module



Modern Cryptography

Bit: Basic data type in computing where there are only 2 possible values for each digit (1 or 0)

Recall the chapter on Booleans! It's a similar concept!

Modern Cryptography

The ciphers still take **data** and **transform** it to **ciphertext** through a series of mathematical functions **based on a key**

The main difference is that the data is **binary** instead of textual

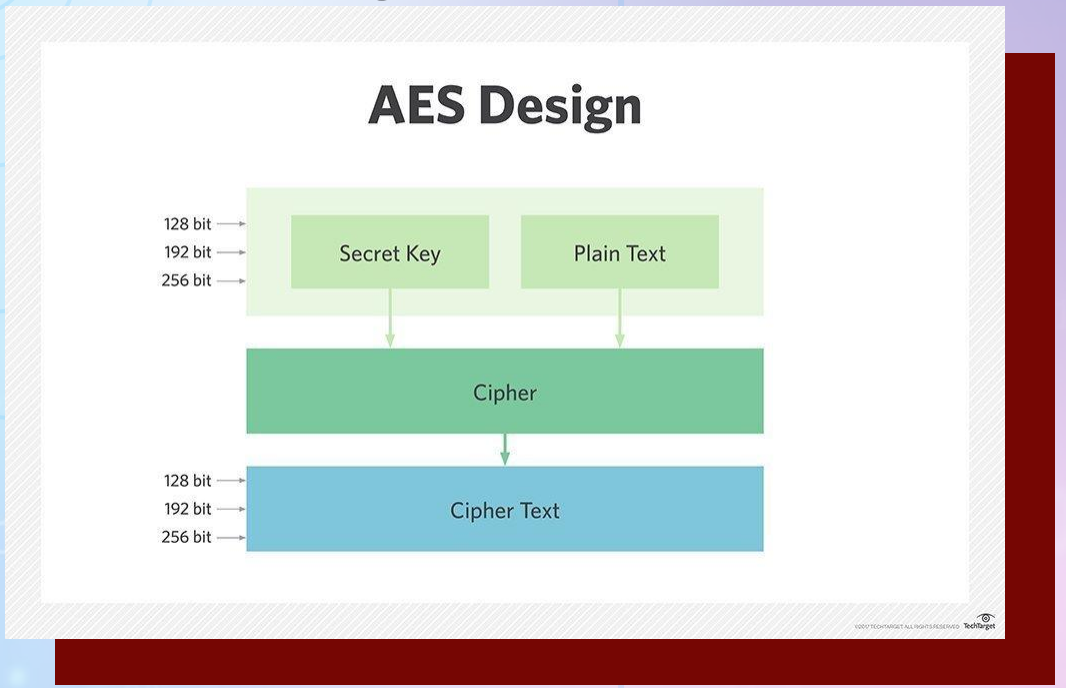
10101
01011
10101

vs

AES

AES – Advanced Encryption Standard

Key length of: 128, 192 or 256 bits

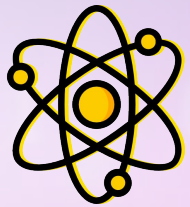


How safe is AES 256?

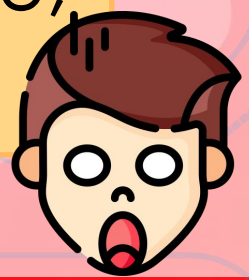
AES

256 bits means 2^{256} different combinations

That's more than the number of atoms in the entire universe.



2^{256} = 115, 792, 089, 237, 316, 195, 423, 570, 985, 008, 687, 907, 853, 269, 984, 665, 640, 564, 039, 457, 584, 007, 913, 129, 639, 936

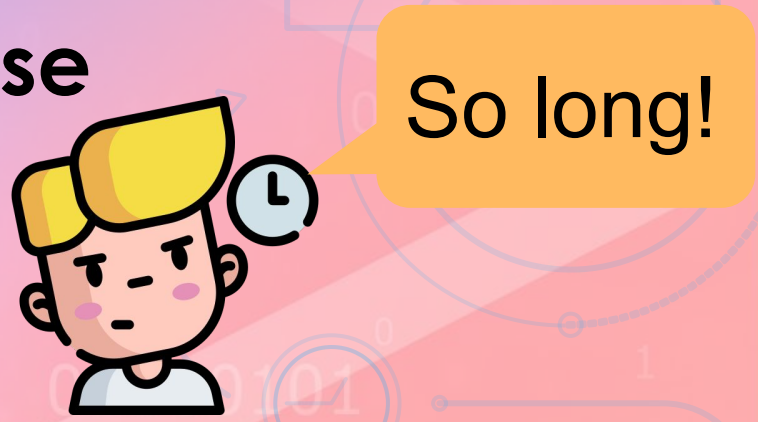


Brute Force?

How long would it take to brute force an AES 256 key?

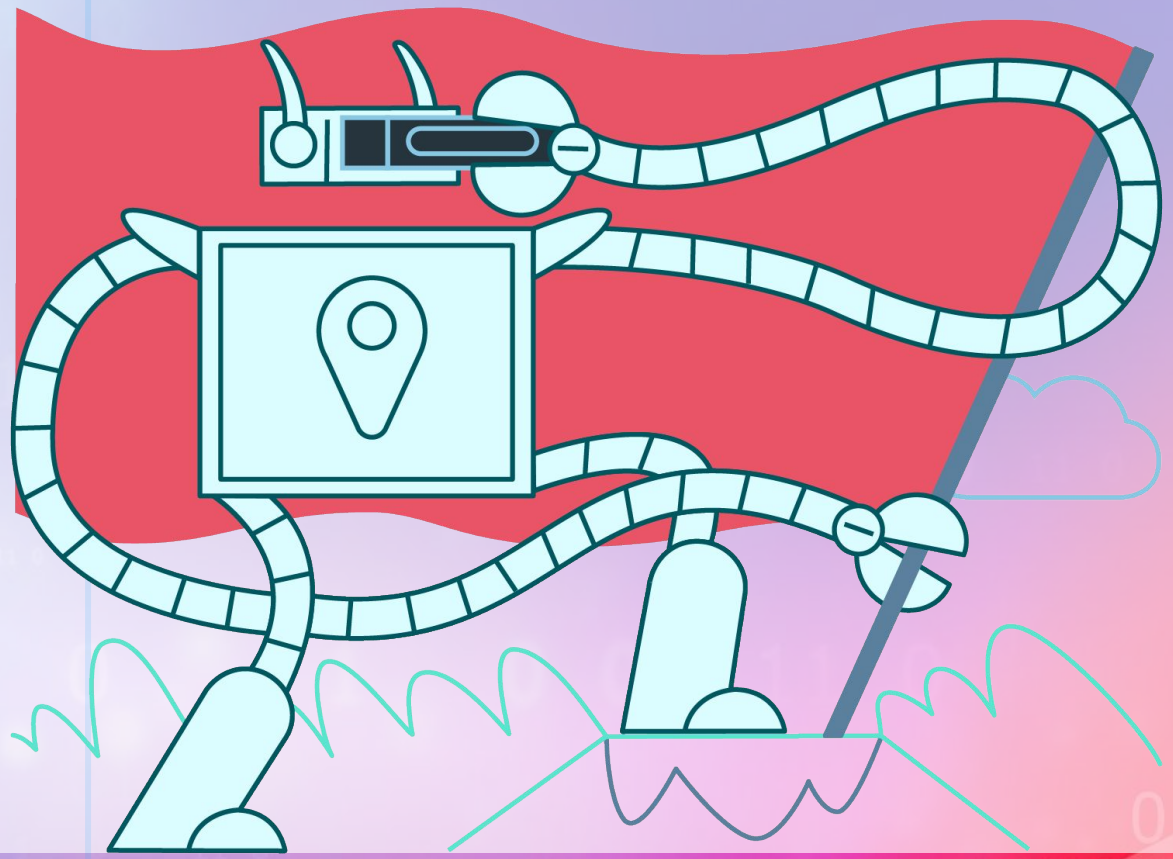
Well, if **every atom on earth** was a computer that could try **1 billion keys per second**, it would still take **longer than the age of the universe**

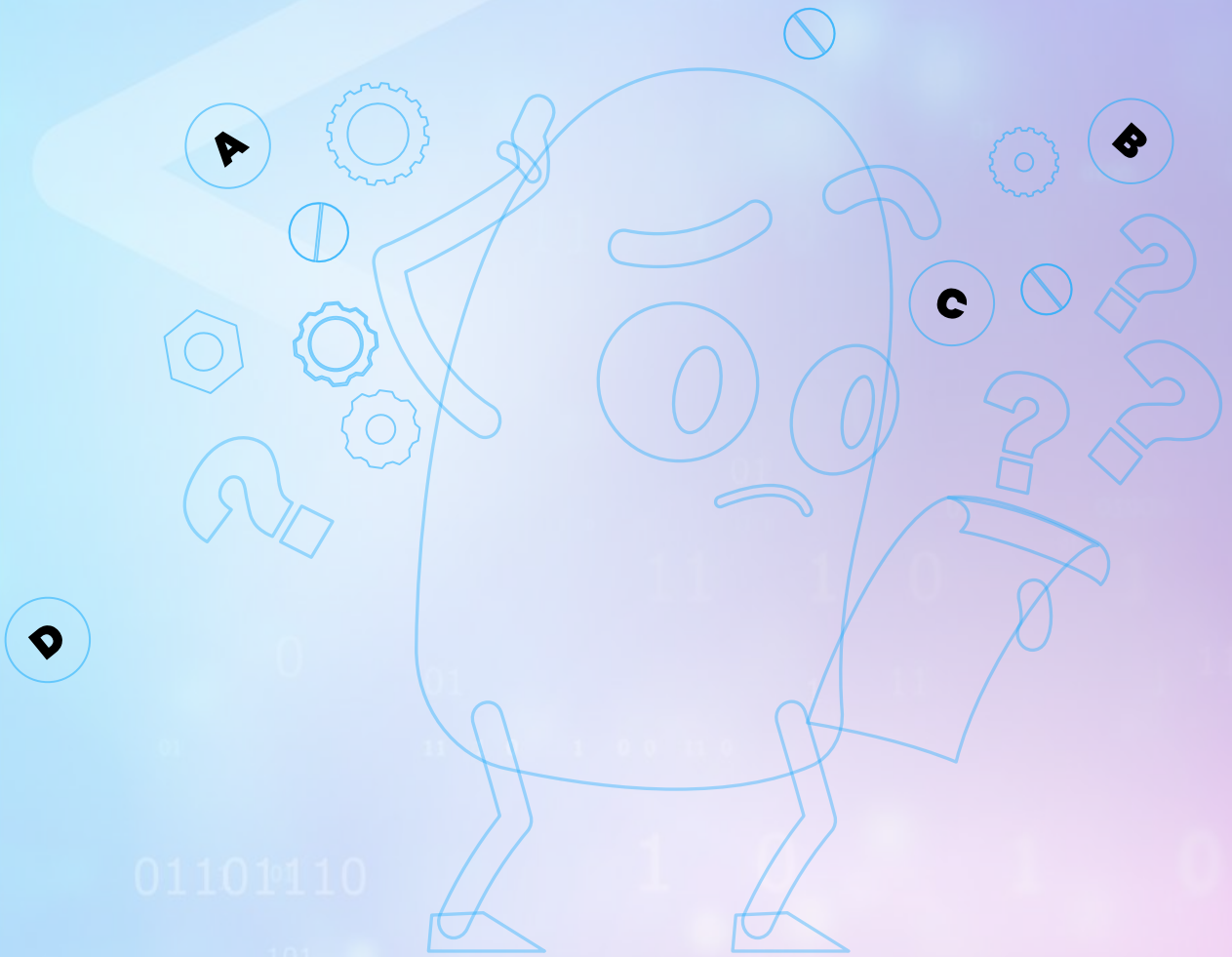
Yeah... No.



More about AES

Demo - AES





Questions?

Sentinel

Your Turn!

> Play around, have fun, ask questions!